FISMA IMPLEMENTATION PROJECT
Phase II

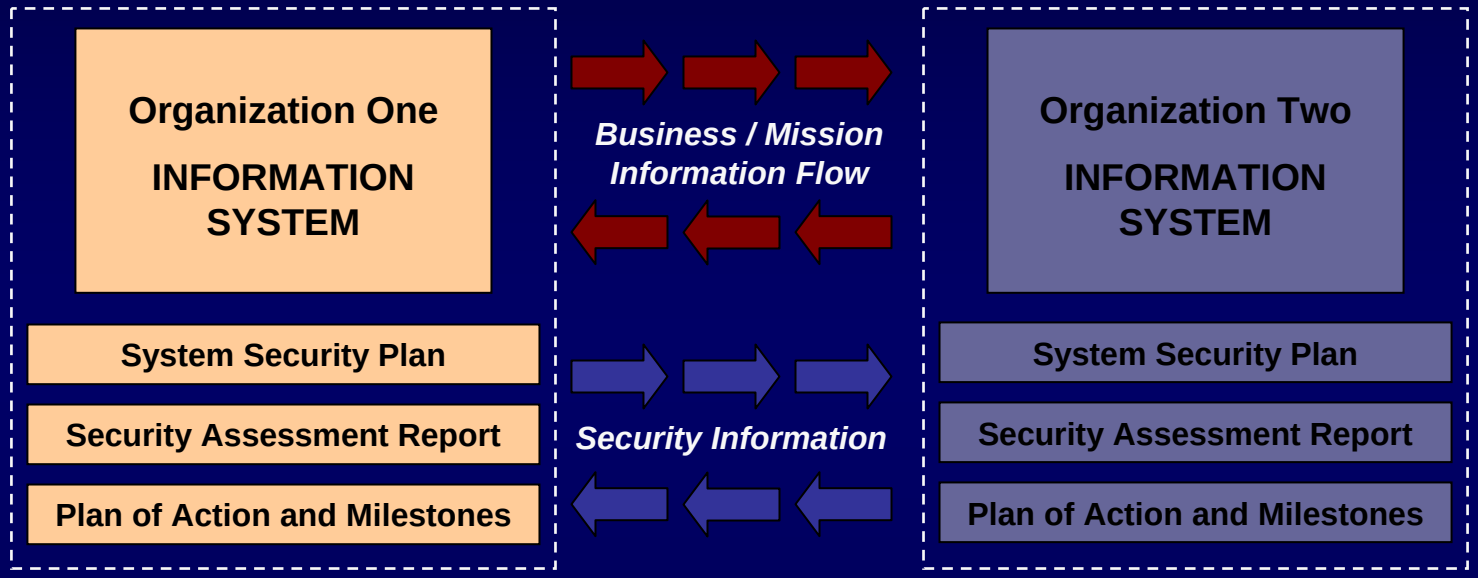
March 13, 2008

Pat Toth

Computer Security Division
Information Technology Laboratory

Trust Relationships

Security Visibility Among Business/Mission Partners



Determining risk to the organization's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the nation; and the acceptability of such risk.

The objective is to achieve *visibility* into prospective business/mission partners information security programs…establishing a trust relationship based on the trustworthiness of information systems.

Agenda

- FISMA Phase I
  - *What we have accomplished to date…*
- FISMA Phase II
  - *Where we are headed …*
- Discussion

FISMA Phase I Publication Status

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (Risk Management) **
- NIST Special Publication 800-37 (Certification & Accreditation) *
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment) **
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping) *

* Publications currently under revision.
** Publications currently under development.

FISMA Phase II

- Mission: Develop and implement a harmonized standards-based organizational credentialing program, supported by tools (automated where possible), and training for public and private sector entities to demonstrate core competencies for offering security services to federal agencies.
- Timeline: 2007-2010
- Status: Initial work began late 2007.

FISMA Phase II Goals

- Phase II primarily focuses on FISMA project goals of:
  - More consistent, comparable, repeatable and cost-effective application of security control assessments across the federal information technology infrastructure
  - More complete, reliable, and trustworthy information for authorizing officials--facilitating more informed security accreditation decisions
- Phase II supplemental goals:
  - Suppliers (product and service) [1st party] and customers [2nd party] provide more focused and better defined security control evidence to support information system assessments
  - Assessment providers [3rd party] efficiently acquire and demonstrate competence for assessing security controls in information systems
  - Draw upon, adapt and use available assessment-related standards, guidelines, programs, tools and assessment sources where applicable to optimize assessment effort
  - Converge entire Federal Government on NIST's FISMA-related security Standards and guidelines as the foundation for the entire government

Security Assessments

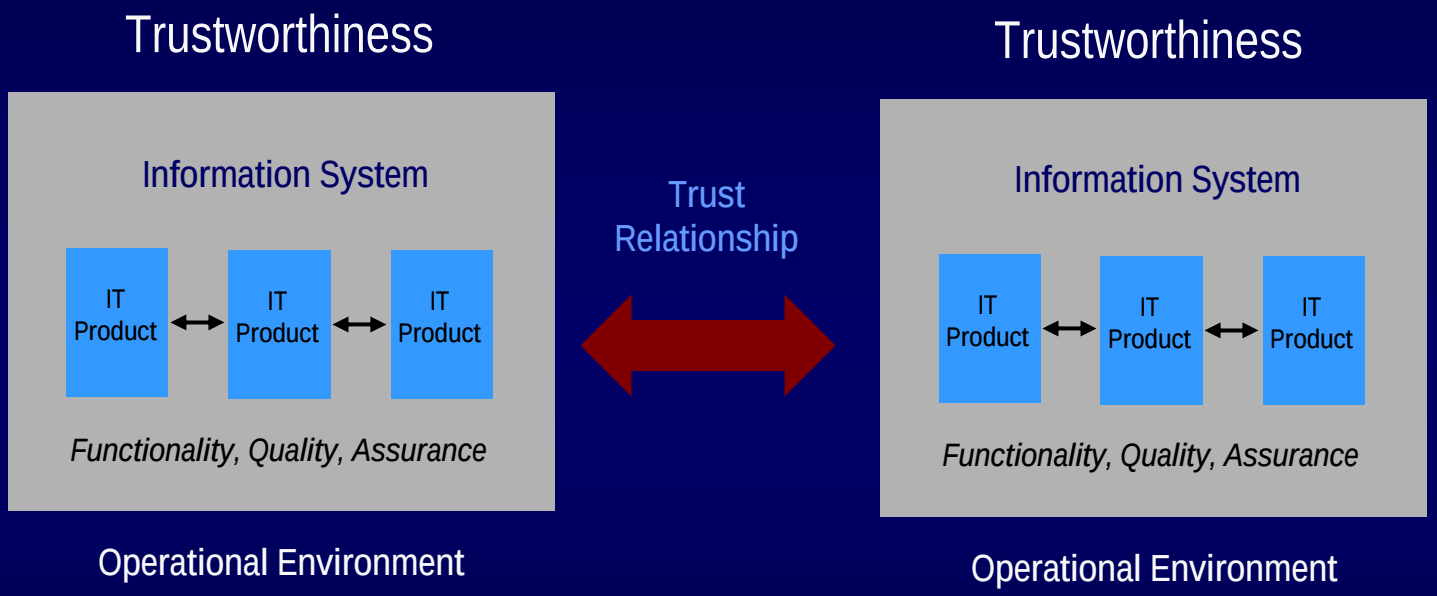
Demonstrating competence to provide information security services including—

- Assessments of Information Systems

  (Operational environments)
  - *Security controls including assurances*
  - *Configuration settings*
  - *Assessments using 800-53A, SCAP and other assessment tools*
  - *Assessment evidence*
- Assessments of Information Technology Products & Services

  (Laboratory environments)
  - *Alternate approaches*
  - *Security functionality (features)*
  - *Security assurance*
  - *Configuration settings*
  - *Assessment evidence*

FISMA Phase II

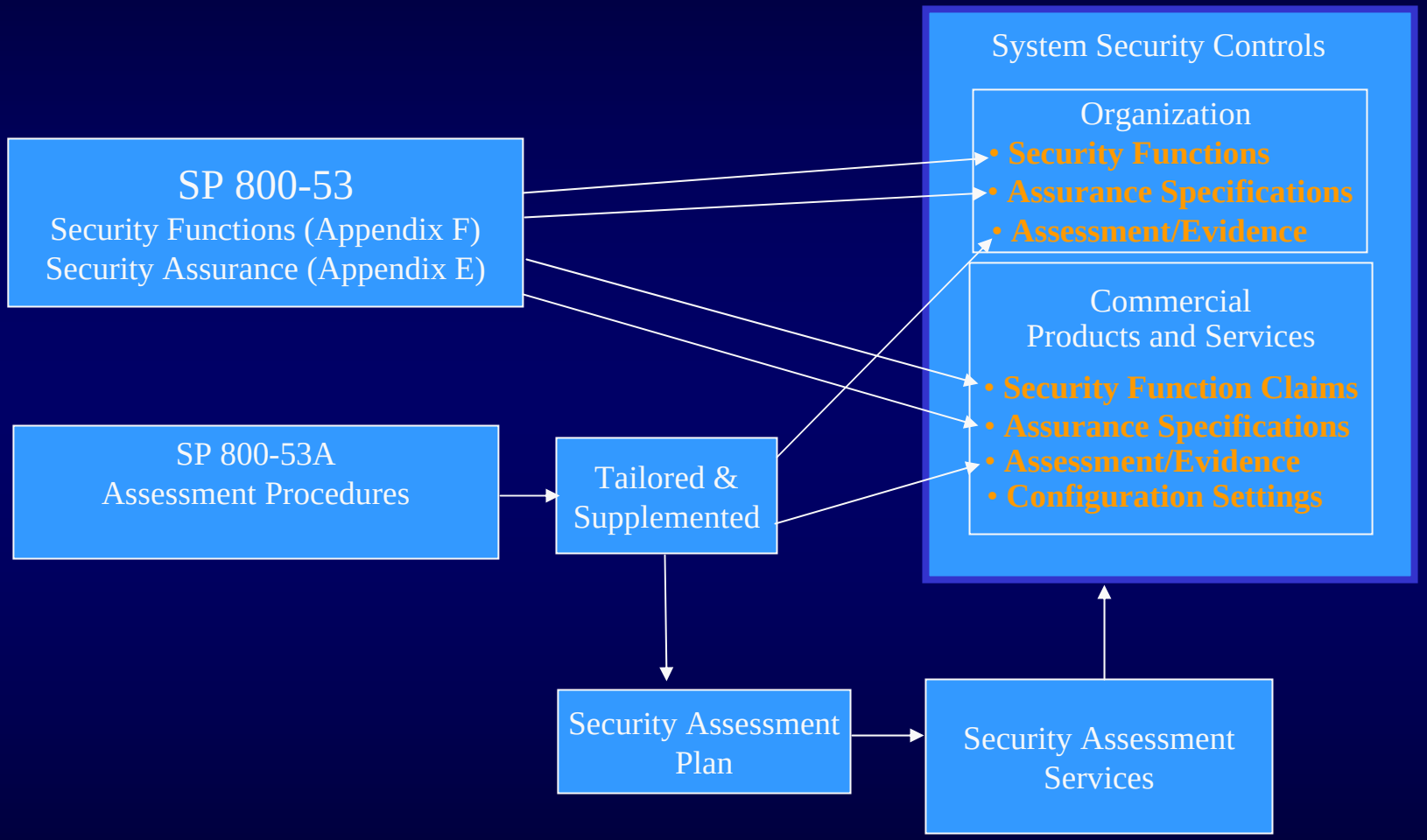


Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.

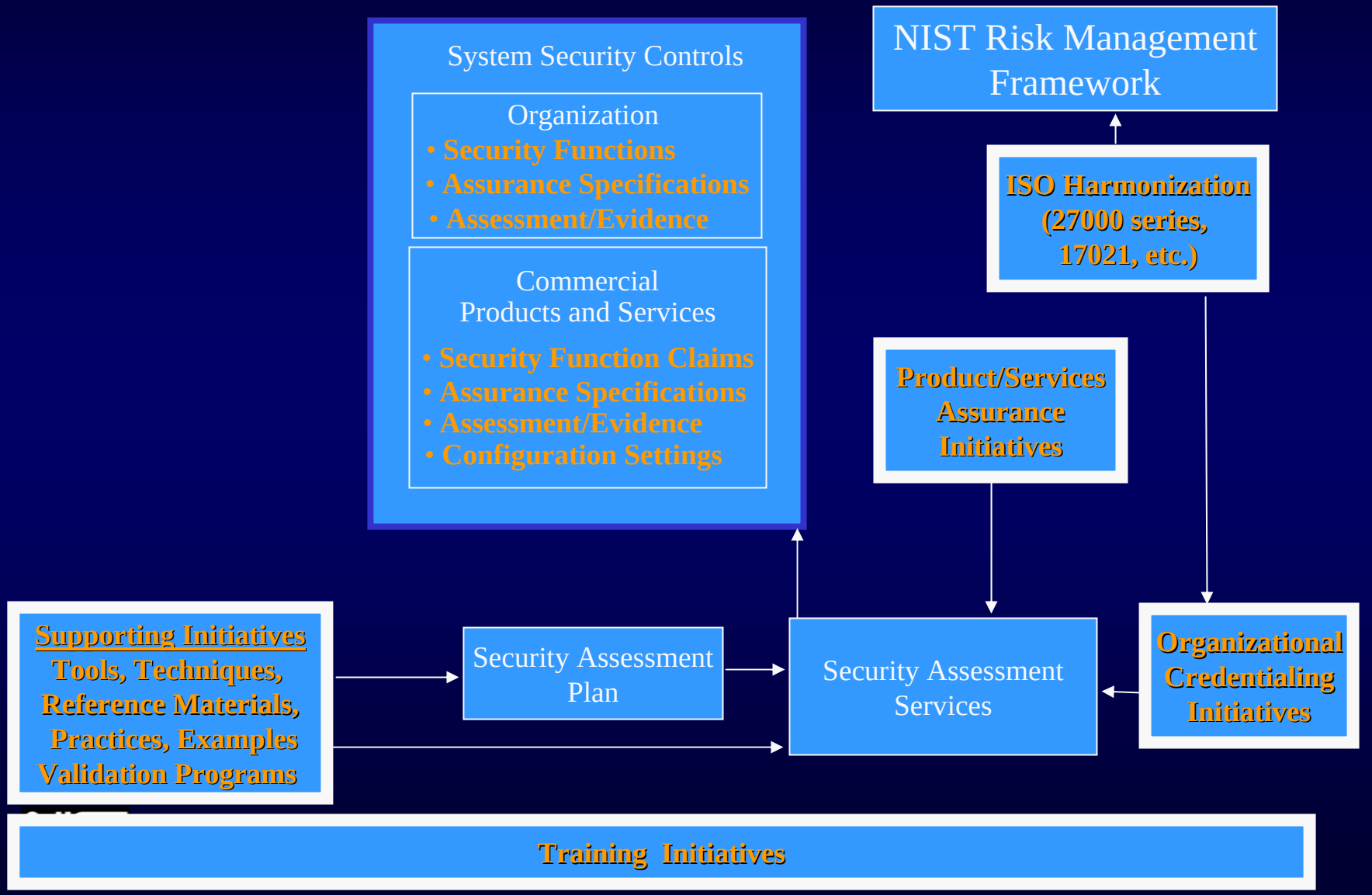
FISMA Phase II Project Initiatives

- Transition – FISMA Phase I to Phase II
- Product and Service Supplier Assurance Initiatives
- Support Tools, Techniques, Reference Materials, Practices & Validation Program Initiatives
- Training Initiatives
- Organizational Credentialing Initiatives
- ISO Harmonization Initiatives

FISMA Phase I to Phase II Transition



FISMA Phase II Initiatives



Product & Service Supplier Assurance

- Security claims specified in terms of:
  - 800-53 security control functions.
  - 800-53 assurance requirements

- Evidence provided to support claims drawing on 800-53A assessment procedures and other assessment processes.

Product & Service Supplier Claims Statement

- NIST define criteria, structure, form, guidelines, etc. for statement.
- Description of security features.
- Identification of 800-53 security controls product/service supported.
- Description of how product or service meets identified security control functional requirements.
- Assurances in context of 800-53 assurance requirements identifying targeted impact level for assurances – e.g., Low impact:
  - How insure obvious errors;
  - How demonstrate feature operates as intended;
  - How insure flaws discovered and addressed in a timely manner.
- Tailoring options for adapting to organization operating environments (e.g., configuration settings).

Product & Service Supplier Claims Statement (cont'd)

- Evidence provided to support claims.
  - Internal assessments reports.
  - External assessments reports (e.g., third party).
  - Government C & A.
- How evidence can be used or tailored to support 800-53A and system specific assessment procedures and processes.

Product & Service Supplier Claims Statement Uses

- Form of assurances that supplier's can readily provide with each product release.
- Base information for including in offers to customers.
- Base information customers can use for assessing product/service acceptance or for conducting supplemental assessments if needed.
- Base information that can be provided to third party evaluators (e.g., validation laboratories) for acquiring additional assurances.
- Base information for system security assessment providers.
- Information for SSP's and Security Assessment Plans.

Identify/Develop Common Assessment Support Tools/References

- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP)
- Cryptographic Module Validation Program (CMVP)
- SCAP Validated Tools
- SP 800-115 Technical Guide to IS Testing
- RMF Standards and Guidelines Quick Start Guides (Summary Sheets), FAQ's …
- Personal Identity Verification Program (NPIVP)
- Etc.

Training Initiatives

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards, guidelines, programs and services.
- Training initiative includes three components—
  - Frequently Asked Questions
  - Publication Summary Guides (Quickstart Guides)
  - Formal Curriculum and Training Courses
- NIST will provide initial training in order to fine-tune the curriculum; then transition to other providers.

Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

Categorize
Information System

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Select
Security Controls

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

Supplement
Security Controls

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Document
Security Controls

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Implement
Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

Assess
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

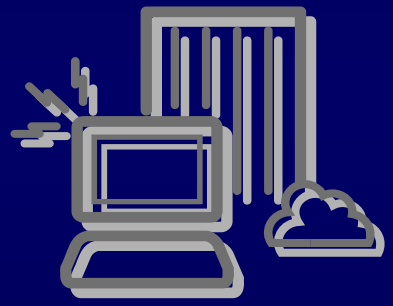
Authorize
Information System

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 800-53A

Monitor
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



Organizational Credentialing Initiatives

- Draft NISTIR 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems* (September 2007).
- Draft Criteria for Product & Service Supplier Claims Statement

Harmonization Initiatives

- Technical: ISO 27000 (Information Security) Harmonization
  - Define relationship between the FISMA security standards and guidelines and the ISO 27001 & 2 Information Security Management System.
  - Provide comprehensive mapping from FISMA standards and guidelines to ISO 27001 & 2.
  - Develop and publish a “delta document” that states commonalities and differences among the standards.
  - Explore possibilities for recognition and acceptance of assessment results to reduce information security costs.
- Organizational: ISO 9000, 17020, 17021, 17024, and 27006 (Management/Quality System, Inspection, System Audit/Certification, Person Certification and Organization Accreditation)
- DNI, DoD, Civilian Agencies

FISMA Phase II
Near Term Tasks and Milestones

- Update Draft NISTIR 7328 based on public comments (March 2008).
- FISMA FAQ's (initial draft April 2008).
- Draft criteria, structure, guidelines, etc. for products and services claiming support of 800-53 security controls (April 2008)
- FISMA Phase II workshop (May 2008)

Longer Term Tasks and Milestones

- Web-based Training Courses – Fall 2008
- In-house training courses – Fall 2008
- Train the Trainers – FY2009
- Credentialing Program – FY2009

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov